

The seal of the Maryland National Guard is a circular emblem. It features a central shield with a yellow field containing a red torch and a blue field containing a white American flag. The shield is flanked by two purple banners. Above the shield is a yellow halo. The entire shield is set against a white background. The seal is surrounded by a green laurel wreath. The words "SERVICE", "INTEGRITY", and "TRUST" are written in white capital letters along the top, right, and bottom of the seal's border, respectively. The word "CANDOR" is written in white capital letters along the left side of the seal's border.

Risk-Based Reviews

**Chief, Internal
Maryland National
Guard**



Risk-Based Reviews



Agenda:

- Risk Definitions
- IIA Standards
- Risk Assessment Process



Risk-Based Reviews



Objectives:

- To show you a process to help perform reviews more efficiently
- To show you how you can also use this process to assist management in accomplishing their risk management requirements



Risk Definitions



Risk - the possibility of an event occurring that will have an impact on the achievement of objectives.
Measured in terms of:

- Impact
- Likelihood



Risk Definitions



Risk Management – A process to identify, assess, manage and control potential risks or situations, to provide reasonable assurance regarding the achievement of the organization's objectives.



Risk Definitions



- Risk Assessment – the identification, measurement and prioritization of risks.
- Two types of risk assessments:
 - Macro
 - Micro



Risk Definitions



Risk Analysis – determining how and when to accept risk.



IIA Risk Standards



2100 – Nature of Work

“The internal audit activity should evaluate and contribute to the improvement of risk management, control and governance processes using a systematic and disciplined approach”.

IIA Standards for the Professional Practice of Internal Auditing



IIA Risk Standards



2110 – Risk Management

“The internal audit activity should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems”.

IIA Standards for the Professional Practice of Internal Auditing



IIA Risk Standards



2110.A1 -

“The internal audit activity should monitor and evaluate the effectiveness of the organization’s risk management system”.

IIA Standards for the Professional Practice of Internal Auditing



IIA Risk Standards



2110.A2 –

“The internal audit activity should evaluate risk exposures relating to the organization’s governance, operations and information systems regarding the:

- reliability and integrity of financial and operational information
 - effectiveness and efficiency of operations
 - safeguarding of assets
 - compliance with laws, regulations and contracts
- IIA Standards for the Professional Practice of Internal Auditing



Internal Review's Risk Role



- Risk analysis, risk assessment and risk management are all part of management's planning tools.
- IR's role is to assist management in assessing risk and its consequences on achieving the organization's goals and objectives.

The seal of the Department of Defense is a circular emblem. It features a central shield with a blue field containing a white eagle with wings spread, perched on a globe. The shield is flanked by two crossed anchors. Above the shield is a banner with the words "DEPARTMENT OF DEFENSE". The entire seal is encircled by a ring containing the words "SERVICE", "INTEGRITY", and "TRUST" at the top, and "CANON" at the bottom. The seal is surrounded by a wreath of olive and oak branches.

Risk Assessment Process



Risk Assessment Process



1. Identification
2. Measurement
3. Prioritization



Risk Identification



Three types of approaches:

1. Exposure Analysis
2. Environmental Analysis
3. Threat Scenarios



Exposure Analysis



Managers put assets at risk to achieve the organization's objectives:

- Financial assets (cash, funding)
- Physical assets (real property, equipment)
- Human assets (personnel)
- Intangible assets (information, reputation)



Exposure Analysis



The Exposure Analysis works best on business processes that are resource-intensive.

Examples:

- Manufacturing or construction processes (physical assets)
- MWR, NAFI activities (financial assets)
- Depots, Motor Pools (physical and human assets)
- Inventory processes (physical assets)
- RTDE (human, intangible and financial assets)
- Information Systems (intangible and human assets)



Exposure Analysis



The Exposure Analysis evaluates the:

- Size
- Type
- Portability
- Location

of the assets involved in the particular business process.




Exposure Analysis



Process:

1. Identify the major assets by size, type, portability and location.
2. Brainstorm with functional area personnel to determine how each of the assets are exposed to loss of value or impairment/loss of utility in relation to accomplishing the goals and objectives



Practical Exercise – Exposure Analysis



Exposure Analysis



Practical Exercise: Motor Pool Operations

1. Identify the major assets by size, type, portability and location.
 - Financial
 - Physical
 - Human
 - Intangible



Exposure Analysis



Practical Exercise: Motor Pool Operations

2. Brainstorm to determine how each of the assets are exposed to loss of value or impairment/loss of utility in relation to accomplishing the goals and objectives



Exposure Analysis

PE: Motor Pool Operations



Asset	Risks of Loss	Risks of Impairment



Exposure Analysis



A possible solution: Motor Pool Operations

1. Identify the major assets by size, type, portability and location.
 - Financial – repair parts budget, GPC
 - Physical – vehicles, maintenance equipment, office equipment
 - Human – mechanics, drivers, office staff
 - Intangible – customer service, reputation



Exposure Analysis

A possible solution: Motor Pool

Operations

Asset	Risks of Loss	Risks of Impairment
Office equipment (small, portable, valuable)	Theft, fire, flood	Equipment malfunction, power outage
Repair parts (small, portable, valuable)	Theft, misappropriation	Defective, malfunction
Vehicles (large, portable, valuable)	Theft, fire, accident	Accident, malfunction
Human (mechanics, office staff)	Accident, ETS, PCS	Accident, illness
Repair parts budget (fixed, valuable)	Fraud, waste, abuse	Waste, budget cuts
GPC (small, portable, valuable)	Theft, fraud	Budget cuts
Customer service (intangible)	Outsourcing	Personnel shortages
Reputation	Accidents, violations	Accidents, timeliness



Environmental Analysis



The Environmental Analysis evaluates risk within organizations and entities which exist in an environment made up of many other external environments:

- Physical – site, location, weather, terrain, access
- Economic – finances, general economy
- Government – laws, policies, regulations
- Competition
- Constituents/customers – internal and external
- Suppliers – internal and external
- Technology

It considers risk arising from the state of these other environments, both current and future.



Environmental Analysis



The Environmental Analysis works best in service-oriented processes, or those that are highly regulated or competitive. Examples:

- Sales, marketing and distribution functions
- Bank operations
- Customer service activities
- **Government**
- Public utilities
- Internal service functions (personnel, legal, accounting, etc.)



Environmental Analysis



Process:

1. From the list of environments, determine which impact the particular business process/entity under review.
2. Brainstorm with functional area personnel to determine the current state of each environment, and identify future changes which would negatively impact customer service goals and objectives.



Practical Exercise - Environmental Analysis



Environmental Analysis



Practical Exercise: Motor Pool Operations

1. Determine which environments impact the particular business process/entity under review:

Physical – site, location, weather, terrain, access

Economic – finances, general economy

Government – laws, policies, regulations

Competition

Constituents/customers – internal and external

Suppliers – internal and external

Technology



Environmental Analysis



Practical Exercise: Motor Pool Operations

2. Brainstorm to determine the current state of each environment, and identify future changes which would negatively impact customer service goals and objectives.



Environmental Analysis

PE: Motor Pool Operations



Environment	Current Environment	Future Environment



Environmental Analysis



A possible solution: Motor Pool Operations

1. Determine which environments impact the particular business process/entity under review:

Economic – finances, general economy

Competition – outsourcing

Customers – internal

Suppliers – external

Technology



Environmental Analysis

A possible solution: Motor Pool

Operations

Environment	Current Environment	Future Environment
Economic	Vulnerable to price changes	Increased fuel costs, or fuel shortages
Competition	Vehicle maintenance routinely done in-house	Push to privatize and/or outsource vehicle maintenance
Internal customers	Customers expect and demand certain levels of service	Increased demands for service (OPTEMPO)
External suppliers	Many local suppliers of repair parts, parts available	Repair parts become in short supply due to increased OPTEMPO
Technology	Vulnerable to system or equipment malfunction	Increased vulnerability of system or equipment malfunction as it ages



Environmental Analysis



Caveats:

- Environmental Analysis is more subjective than Exposure Analysis.
- Brainstorming involves a wide range of subjects, so it is best done with management and/or subject matter experts within the area under review.
- Start a risk analysis with either the Exposure Analysis or the Environmental Analysis and then do the other to fully identify significant risks.



Threat Scenarios



- Threat Scenarios are descriptions of the business process and the assets at risk, as well as potential consequences.
- Can include description of mitigating control(s), as well.



Threat Scenarios



- Most useful when dealing with fraud or security issues.
- Often used after performing either or both of the other two Risk Assessment analyses.
- Are a subset of the Exposure Analysis, but focus on fraud and disaster.
- Require significant time and skill to do properly and thoroughly.



Threat Scenario



Process:

- Business process is carefully documented
 - narrative form
 - portfolio form – preferred method



Threat Scenario



Portfolio Description Example:

- Asset Description:
 - Mainframe computer
- Specific Threat:
 - Water damage
- Consequences of Threat to Asset:
 - System “down-time”, repair/replacement costs, loss of data
- How threat is typically realized:
 - Roof leaks, flooding



Threat Scenario



If the purpose of the scenario is to assess the risk of fraud, the “how realized” portion of the Portfolio Description should cover the three elements of fraud:

- Theft – how the asset could be stolen
- Concealment – how the theft could be concealed or go undetected
- Conversion – how the assets could be converted to personal use



Threat Scenario



Once the risks are identified, the evaluator looks for controls that are missing and designs tests to ensure that other controls are working as intended.



Risk Identification - Summary



Successful risk identification requires two things:

1. a thorough understanding of the entity (macro), and the major business process being reviewed (micro), and
2. a methodology to generate a reasonable list of potential risks



Risk Identification - Summary



- Identify the assets, and potential losses/impairments to them (exposure)
- Identify the services we provide with those assets and what could prevent us from providing the service (environmental)
- Identify situations where a specific business process is vulnerable to fraud or disaster (threat scenario)



Measuring Risk



- After identification, the next step is to measure risks.
- Measuring risk is difficult, because of its intangible nature.
- Can be measured quantitatively (ex. probability estimates)
- Qualitative terms most often used to describe risk (High, Medium, Low)



Measuring Risk



Methods for measuring risk:

- Direct probability estimates and expected loss functions.
- Risk factors.
- Weighted or sorted matrices.



Measuring Risk



Risk Factors:

- Favored for macro risk assessments
- Not efficient for micro risk assessments, except when the reviewable entities are uniform throughout the organization



Measuring Risk



Risk Factors:

- Aid in measuring the risk in the review/audit universe
- Factors chosen that apply to all/most reviewable entities
- Some factors are more important, and are weighted



Measuring Risk



Three Types of Risk Factors:

1. Subjective

- Integrity of management
- Extent of changes in business processes

2. Objective or historical

- Dollars at risk (objective)
- Employee turnover rates (historical)

3. Calculated

- Distance from headquarters
- Time since last review



Measuring Risk



Minimizing Bias in Risk Factors:

- Objective, Historical and Calculated risk factors are easily measured – quantitative.
- Subjective risk factors are not as easily quantified. Two methods used to minimize bias:
 1. Intuition
 2. Collaborative (group) processes



Measuring Risk



Minimizing Bias in Risk Factors:

- Intuition
 - experienced evaluators can use to arrive at reasonable estimates of risk
 - measurement must be done on-site, so that full range of influence can be perceived



Measuring Risk



Minimizing Bias in Risk Factors:

- Collaborative Group Techniques:
Group decision tools allow the evaluator to pool the experience and intuition of a larger group of experts:
 - Delphi Technique
 - Control Self Assessment
 - Modified Delphi Technique



Measuring Risk



Minimizing Bias in Risk Factors:

- Delphi Technique:
 1. Panel of “experts”
 2. List of items to be assessed
 3. Individuals privately rank
 4. Lists turned into coordinator
 5. Coordinator compiles composite list
 6. Composite and original given back to each panelist
 7. Panelists compare their list to composite, make adjustments
 8. Repeat steps 3 thru 7 until consensus reached



Measuring Risk



Minimizing Bias in Risk Factors:

- Modified Delphi Technique: much the same as the Delphi Technique, except:
 - Individuals all in same room at same time
 - Lists are not private
 - Composite list posted, argued/discussed until consensus reached
- Caveat:
 - Quicker, but subject to more bias (rank and/or strong personalities)



Measuring Risk



Weighted or sorted matrices:

- Most effective for micro risk assessments
- Similar to using risk factors:
 - uses reviewable entity components
 - weights certain factors
- Differences:
 - format (matrices)
 - risks pre-defined
 - can look at risks over multiple time periods
- Uses threats versus components matrices to evaluate consequences and controls



Prioritizing Risk



Three methods of prioritizing risk:

1. Absolute ranking
2. Relative ranking
3. Matrices Ranking



Prioritizing Risk



1. Absolute ranking

- Risks and consequences identified and measured
- Components ranked by their scores:
 - Total score
 - Proportional ranking
 - Average ranking (not a common method)



Prioritizing Risk



1. Absolute ranking

- Total score: ranked in order of magnitude
- Proportional ranking:
 - the individual components' total scores are converted into a percentage of all scores
 - useful for allocating review/audit budget over the entity's components)
- Average ranking:
 - the individual components' total scores are converted into an average risk score by dividing the total by the number of risk factors
 - adds no real value to the planning decision



Prioritizing Risk



2. Relative ranking

- Risks and consequences identified and measured
- Scores grouped into pre-defined ranges or natural clusters (High, Medium, Low risk)
- Sufficient for general planning purposes



Prioritizing Risk



2. Relative ranking

- Direct calculation:
 - Pre-defined ranges (ex. < 20 = Low, $20-39$ = Medium, $40+$ = High)
 - Cluster ranges – not pre-defined. Values examined for gaps, and clusters labeled Low, Medium, High



Prioritizing Risk



2. Relative ranking

- Pattern matching:
 - The scores of each factor are significant, rather than the total score
 - The pattern determines the overall risk classification
 - The difference in significance or consequences of different risk factors is handled by weighting the factors



Prioritizing Risk



2. Relative ranking

- Normative tables:
 - Component's risks are not measured numerically
 - Classified using a descriptive model (measurement table)
 - Measurement table usually includes descriptions of risk and controls
 - The combinations of risks and controls equate to levels of testing required



Prioritizing Risk



3. Matrices Ranking

- A form of relative ranking
- Combines risk measurement and risk prioritization into one process.
- Uses a matrix of threats vs. reviewable unit components
- Axes are sorted so that natural quartiles identify High, Medium Low risk



Risk-Based Reviews



Risk Assessment in the Review Process:

- Macro
- Micro



Risk-Based Reviews



Macro Risk Assessment:

- used to create the Annual Program/Schedule
- identifies reviewable areas of greatest significance within the organization



Macro Risk Assessment



1. Define the review universe (auditable entity file)
2. Identify the major risks
3. Translate risks into measurable risk factors
4. Choose weights for risk factors
5. Establish scoring mechanism for each risk factor
6. Score factors for each reviewable entity
7. Sort reviewable entities by total risk score
8. Develop Annual Plan based on the ranked



Macro Risk Assessment



RISK FACTORS

1. Relationship to organizational mission: H = critical.
2. Program/system performance level: H = performance is below established standards.
3. Program complexity: H = complex.
4. Vulnerability to adverse public opinion: H = very vulnerable.
5. Degree of external/Congressional interest: H = Congressional interest.
6. Adequacy or effectiveness of internal control systems: H = weak/ineffective controls.
7. Vulnerability to waste, fraud or mismanagement: H = very vulnerable.
8. Age of program/system or major changes: H = program or system age is a risk factor.
9. History of major deficiencies: H = yes.
10. Previous audit/inspection coverage: H = little or no coverage during audits/inspections.
11. Financial exposure: H = high dollar value of assets or funding provided.
12. Ethical climate: H = history of "questionable" transactions, "bending" the rules, etc.
13. Competence of personnel and/or adequacy of staffing: H = significant or key personnel turnover or inadequate staffing to accomplish missions or functions.
14. Time since last audit/inspection: H = 5 years or more since last audit/inspection.
15. Management special requests for audit: H = Commanding General or Senior Leadership special request.



Risk-Based Reviews



Micro Risk Assessment:

- used to identify areas within the scope of the review that are most important
- tests the most important controls, or
- tests the controls in more depth



Micro Risk Assessment



1. Define the business objectives for the area under review
2. Describe the major components/assets of the entity that help achieve the objectives
3. Speculate on risks or threats to achieving the objectives
4. Develop a matrix of components/assets on the left axis and threats/risks on the top axis
5. Sort the two axes from highest to lowest
6. Divide the matrix into quartiles
7. Design the review program based on risk

The seal of the Department of Defense is centered in the background. It features an eagle with a shield, holding an olive branch and arrows, with a constellation of stars above its head. The seal is encircled by a ring containing the words "SERVICE", "INTEGRITY", and "TRUST".

Risk-Based Review Process



Micro Risk Assessment PE – XYZ Logistics Agency



1. Define the business objectives for the distribution process of the XYZLA:
 - a. XYZLA's mission statement is "to provide customers with world-class products that meet their needs"
 - b. The mission statement of the Distribution Branch of XYZLA is "to ensure that products reach customers in the required quantities, at the required locations, on time, every time"

Step 1 – Risk Identification



Micro Risk Assessment PE – XYZ Logistics Agency



1. The link between the business objectives for XYZLA and its distribution process is customer service. This will be the focus of the review.

Step 1 – Risk Identification



Micro Risk Assessment PE – XYZ Logistics Agency



2. Describe the major components/assets of the entity that help achieve the objectives (examples: key processes, functions, positions, workgroups, major assets, etc.)
 - a. List the components/assets necessary to achieving XYZLA's goals and objectives.
 - b. Reduce the list to the six or eight most important

Step 2 – Risk Identification



Micro Risk Assessment PE – XYZ Logistics Agency



Major components/assets of the entity:

1. Warehouse
2. Inventory
3. Stockmen
4. Packers
5. Shippers
6. Trucks
7. Truck Drivers
8. Forklifts
9. Truck routing software
10. Order entry software
11. Inventory/reorder software

Step 2 – Risk Measurement



Micro Risk Assessment PE – XYZ Logistics Agency



Most important components/assets of the entity:

1. Warehouse
2. Inventory
3. Warehousemen
4. Trucks
5. Truck Drivers
6. Inventory/reorder software

Step 2 – Risk Measurement



Micro Risk Assessment PE – XYZ Logistics Agency



3. Speculate on risks or threats to achieving the goals and objectives, using one of the three risk identification analyses (Exposure, Environmental, Threat)
 - a. Brainstorm to think of obstacles to accomplishing the goals and objectives
 - b. Reduce this list to the six or eight most important

Step 2 – Risk Measurement



Micro Risk Assessment PE – XYZ Logistics Agency Exposure Analysis



Asset	Risks of Loss	Risks of Impairment
Warehouse (large, non-portable, valuable)	Fire, flood, other natural disaster	Flood, power outage
Inventory (varied, portable, valuable)	Fire, flood, other natural disaster, theft	Damage, obsolescence
Human (Warehousemen)	Death, major accident or injury	Illness, minor accident or injury
Trucks (large, portable, valuable)	Fire, theft, accident (major)	Accident (minor), malfunction
Human (Truck drivers)	Death, major accident or injury	Illness, minor accident or injury
Inventory/reorder software (intangible)	Computer virus, system crash	Power outage, computer virus

Step 2 – Risk Measurement



Micro Risk Assessment PE – XYZ Logistics Agency Environmental Analysis



Environment	Current Environment	Future Environment
Economic	Relatively stable inventory costs	Increased inventory costs, or inventory shortages
Competition	None -central distribution facility for 1 st US Army	Increased use of GPC, JIT inventories
Internal customers	Customers expect and demand certain levels of service	Increased demands for service (OPTEMPO)
External suppliers	Many local suppliers of inventory available	Inventory becomes in short supply due to increased OPTEMPO
Technology	Software vulnerable to system or equipment malfunction, power outages	Increased software vulnerability due to system or equipment malfunction as it ages

Step 2 – Risk Measurement



Micro Risk Assessment PE – XYZ Logistics Agency



From the analyses, develop a list of the most significant components/assets and threats/risks:

Components/Assets	Threats/Risks
Warehouse	Fire
Inventory	Theft
Warehousemen	Accident
Trucks	Injury
Truck Drivers	Inventory Shortage
Inventory/Reorder software	System Crash

Step 2 – Risk Measurement



Micro Risk Assessment PE - XYZ Logistics Agency



4. Develop a matrix of components/assets on the left axis and threats/risks on the top axis **Threats/Risk**

**C
o
m
p
o
n
e
n
t
s**

	S Fire	Theft	Accident	Injury	Inventor y Shortage	System Crash
Warehouse						
Inventory						
Warehouse -men						
Trucks						
Truck Drivers						
Inventory Software						



Micro Risk Assessment PE – XYZ Logistics Agency



Working with management and/or subject matter experts, rank order the components/assets and

Components/Assets	Ranking	Threats/Risks	Ranking
Warehouse	6	Fire	4
Inventory	1	Theft	2
Warehousemen	3	Accident	3
Trucks	2	Injury	6
Truck Drivers	4	Inventory Shortage	1
Inventory/Reorder software	5	System Crash	5

Step 2 – Risk Measurement



Micro Risk Assessment PE – XYZ Logistics Agency



5. Sort the two axes (components/assets and threats/risks) from highest to lowest:

Hig **Threats/Risk** **Lo**
h **s** **w**

Hig
h

C
o
m
p
o
n
e
n
t
s

Lo
w

	Inventor y Shortag e	Theft	Acciden t	Fire	System Crash	Injury
Inventory						
Trucks						
Warehous e men						
Truck Drivers						
Inventory Software						
Warehous e						

Step 2 – Risk Measurement



Micro Risk Assessment PE – XYZ Logistics Agency



Working with management and staff, examine each threat/component combination and determine if the controls over each threat against each component are Strong (S), Weak/Missing (W), or not known (Blank).

Step 3 – Risk Prioritization



Micro Risk Assessment PE – XYZ Logistics Agency

Post control evaluations on the matrix:

		Threats/Risks					
		High				Low	
High Components Low		Inventory Shortage	Theft	Accident	Fire	System Crash	Injury
	Inventory	W	W		S	W	
	Trucks	S	W	W			
	Warehouse men			W			W
	Truck Drivers			S			S
	Inventory Software	W				S	
	Warehouse				S		

Step 3 – Risk Prioritization

83



Micro Risk Assessment PE – XYZ Logistics Agency



6. Divide the matrix into quartiles:

High Components Low	High	Threats/Risks					Low
		Inventory Shortage	Theft	Accident	Fire	System Crash	Injury
	Inventory	W	W		S	W	
	Trucks	S	W	W			
	Warehouse men			W			W
	Truck Drivers			S			S
	Inventory Software	W				S	
	Warehouse				S		

Step 3 – Risk prioritization



Micro Risk Assessment



7. Design the review program based on risk
 - a. The component/threat cells labeled high risk should be devoted more time/audit testing
 - b. The component/threat cells labeled low risk should be given less emphasis (or none at all)



Risk-Based Reviews Summary



So, what are the advantages of using Risk-Based Reviews?



Risk-Based Reviews Summary



So, what are the advantages of using Risk-Based Reviews?

- IR staff develop a thorough understanding of the business process/entity under review



Risk-Based Reviews Summary



So, what are the advantages of using Risk-Based Reviews?

- IR staff develop a thorough understanding of the business process/entity under review
- IR staff understand the risks and controls in the system



Risk-Based Reviews Summary



So, what are the advantages of using Risk-Based Reviews?

- IR staff develop a thorough understanding of the business process/entity under review
- IR staff understand the risks and controls in the system
- IR staff is used more efficiently




Risk-Based Reviews Summary



So, what are the advantages of using Risk-Based Reviews?

- IR staff develop a thorough understanding of the business process/entity under review
- IR staff understand the risks and controls in the system
- IR staff is used more efficiently
- Value-added reviews/reports



The seal of the Department of Defense is centered in the background. It features an eagle with wings spread, perched on a shield. The shield is divided into four quadrants, each containing a different symbol. The eagle is surrounded by a circular border with the words "SERVICE", "INTEGRITY", and "TRUST" at the top, and "CANDOR" at the bottom. The seal is flanked by two olive branches.

(410) 278-8471
DSN 496-8471